



---

## Bloque IV: El nivel de red

### Tema 9: IP

---

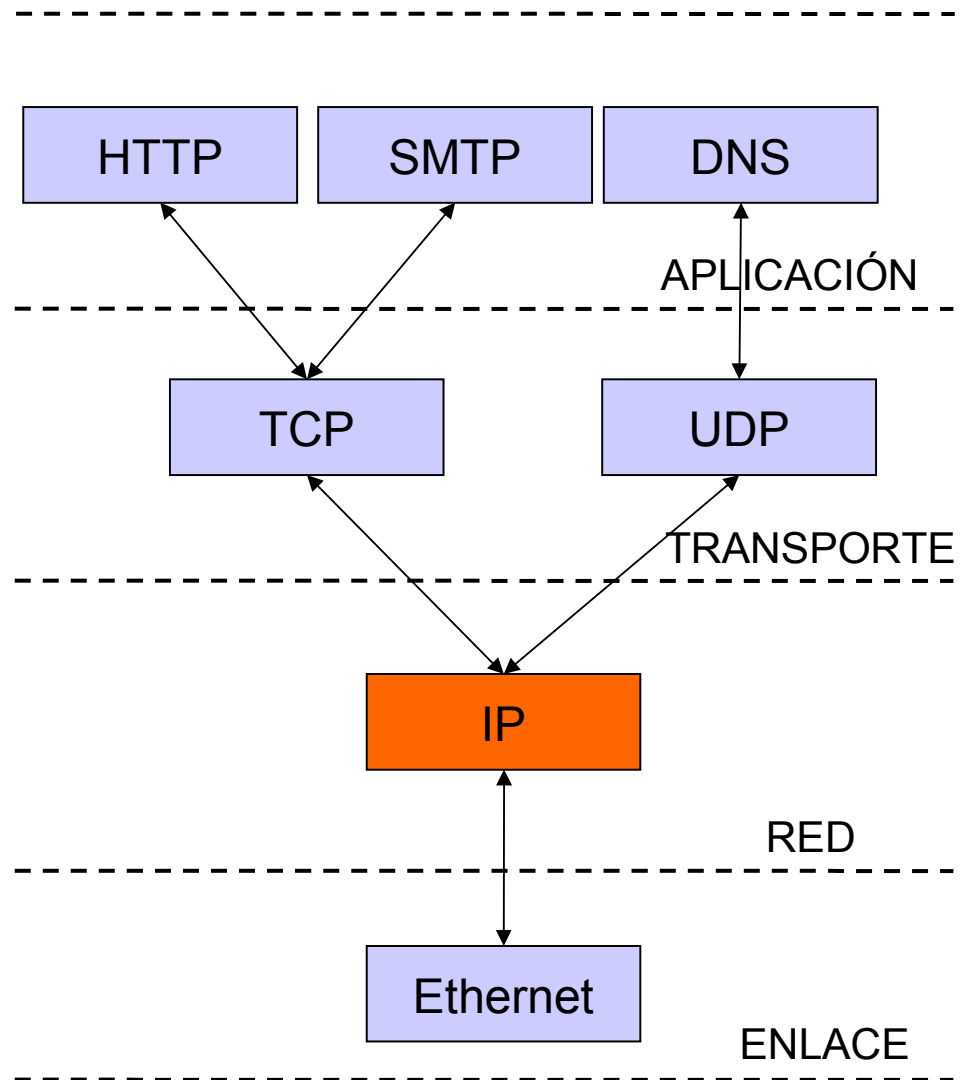


- Bloque IV: El nivel de red
  - Tema 9: IP
    - Introducción
    - Cabecera IP
    - Fragmentación IP
- **Lecturas recomendadas:**
  - Capítulo 4, sección 4.4.1, de “Redes de Computadores: Un enfoque descendente”. James F. Kurose, Keith W. Ross. Addison Wesley.



# Introducción

- Internet Protocolo – Especificado en el RFC 791.
- IP proporciona un servicio de entrega de datagramas **no fiable** y **no orientado a conexión**.





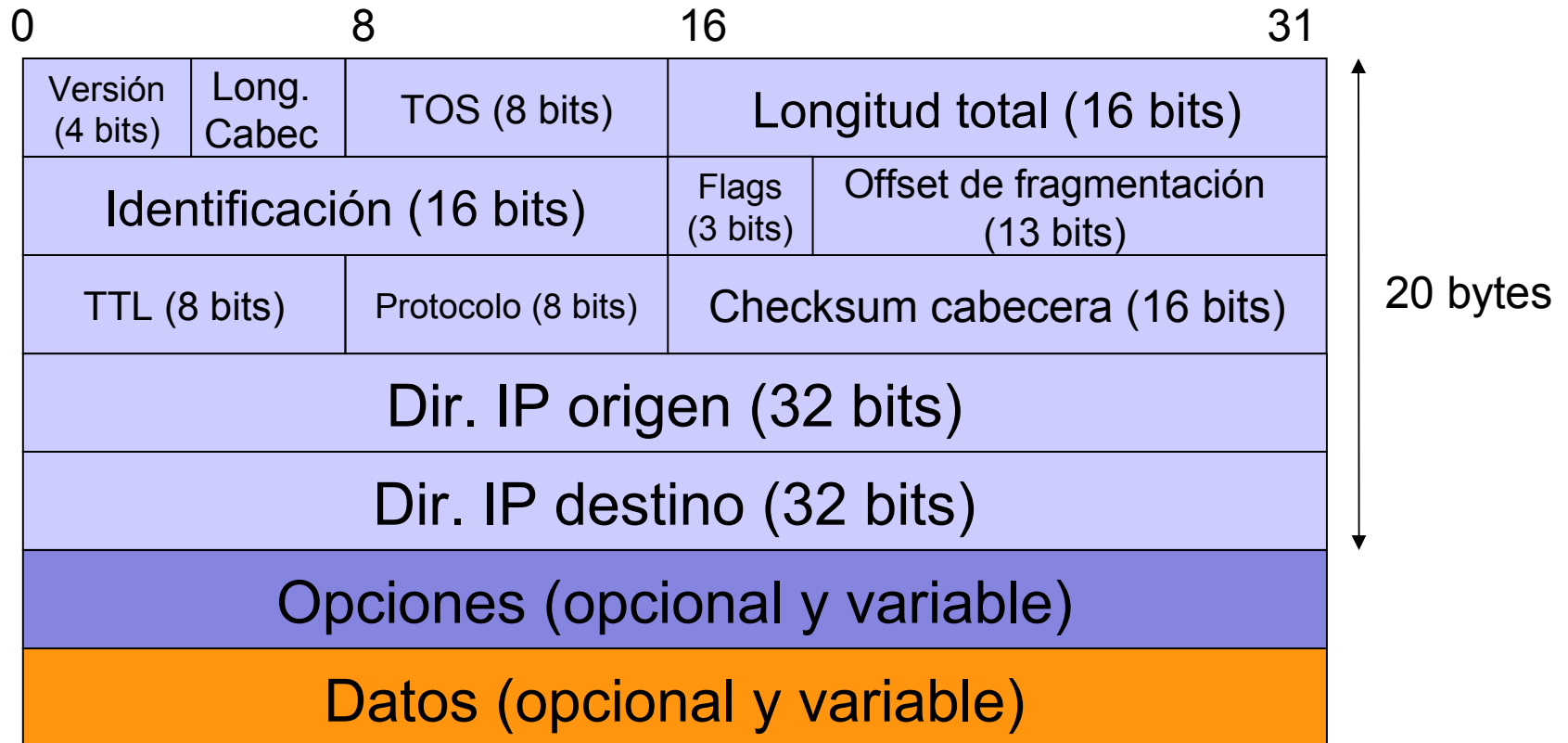
# Introducción

---

- No fiable:
  - No hay garantías de que un datagrama alcance su destino final.
  - IP sigue un modelo “best effort”: lo hará “*lo mejor que pueda*”.
  - En caso de que haya algún problema, IP tiene un sistema de gestión de errores simple: descartar algún datagrama (normalmente el último recibido).
- No orientado a conexión:
  - IP no mantiene información del estado de los datagramas.
  - Cada datagrama es tratado independientemente → Dos datagramas hacia un mismo destino pueden seguir caminos diferentes.
  - Los datagramas se pueden recibir desordenados.



# Cabecera IP





# Cabecera IP

---

- TCP/IP usa la ordenación de bytes “big endian” (de izqda a dcha):
  - Si un equipo usa el formato “little endian” (de dcha a izqda) debe hacer la conversión al transmitir y al recibir.
- **Versión:** Versión actual de IP (4).
- **Longitud de cabecera:** Número de palabras de 32 bits de la cabecera, incluidas las opciones si las hubiera (< 60 bytes).
- **Tipo de servicio (TOS):** diseñado para QoS (Quality of Service), aunque nunca fue ampliamente usado. Redefinido (RFC 2474, 3260) en dos campos:
  - **Servicios diferenciados (DS):** campo de 6 bits utilizado para dar soporte a QoS mediante la técnica de DS.
  - **Explicit Congestion Notification (ECN):** indicador de congestión o futura congestión en un router (2 bits).



# Cabecera IP

---

- **Longitud total:** longitud total de datagrama IP en bytes.
  - Longitud total – longitud cabecera = tamaño datos.
  - Campo de 16 bits: máximo tamaño es 65535 bytes.
  - Muchas aplicaciones limitan actualmente la longitud de los datagramas IP a 8192 bytes (caso de aquellas que utilizan NFS).
  - Se precisa este campo porque un datagrama IP puede llegar a ser de menor tamaño que el mínimo exigido por el nivel de enlace (en Ethernet, el mínimo son 46 bytes de datos). En estos casos se añaden bytes para configurar la trama del nivel de enlace.
- **Identificación:** identifica unívocamente el datagrama IP enviado por una máquina.
  - Normalmente se incrementa en una unidad cada vez que se envía un datagrama.
- **Flags y offset de fragmentación:** Campos para fragmentación.



# Cabecera IP

---

- **TTL (Time To Live):** Establece un tiempo máximo de vida para el datagrama. Previene bucles indefinidos por problemas de enrutamiento.
  - Establece un límite en el número de “routers” por los que puede pasar un datagrama: valor recomendado 64.
  - Cada vez que el datagrama pasa por un “router”, se decrementa en una unidad el valor de este campo.
  - Cuando vale 0 se descarta el datagrama y se notifica al remitente con un mensaje ICMP.
- **Protocolo:** usado por IP para demultiplexar. Permite identificar de qué protocolo de la capa de transporte son los datos enviados.
- **Checksum de cabecera:** sólo para la cabecera. Se calcula:
  - Se pone a cero.
  - Se calcula la suma complemento a uno (en bloques de 16 bits) de la cabecera.
  - El complemento a uno de esta suma se almacena en el checksum.
  - En recepción, se hace la suma complemento a uno de la cabecera. Si no da todos unos, se considera error, se descarta el datagrama y no se notifica.
  - Como cada router decrementa el campo TTL para cada datagrama que enruta, debe actualizarse el checksum.





# Cabecera IP

---

- **Dirección IP de origen y destino:** 32 bits cada una.
- **Opciones:** Información opcional de longitud variable. Algunas opciones son:
  - Registro de enrutamiento (record route): cada router marca su hora y dirección IP (máximo 9 routers).
  - Timestamp: se registra la ruta y además pone una marca de tiempo en cada salto (máximo 4 routers).
  - Lista estricta de enrutamientos (strict source routing): la cabecera contiene la ruta paso a paso que debe seguir el datagrama (máximo 9).
  - Lista difusa de enrutamientos (loose source routing): la cabecera lleva una lista de routers por los que debe pasar el datagrama, pero puede pasar además por otros (máximo 9).
  - NoOp: la longitud ha de ser múltiplo de 32 bits. Esta opción permite añadir bytes de relleno para cumplir esta condición.



# Fragmentación IP

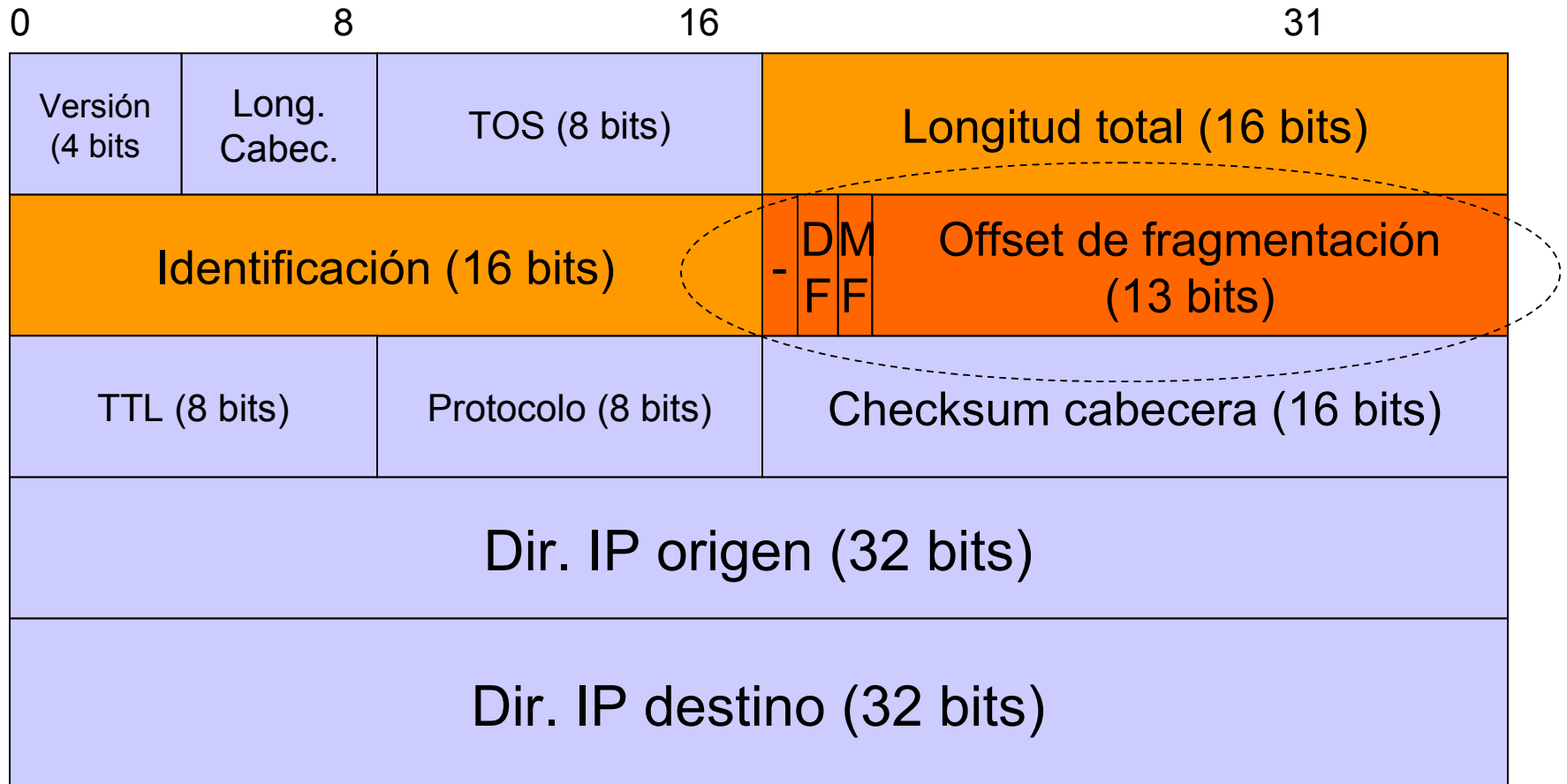
---

- El nivel de enlace de la red impone un límite superior al tamaño de la trama que se puede transmitir (**MTU** – Maximum Transmission Unit: tamaño máximo del campo de datos).
  - Ethernet: 1500 bytes
  - Token Ring: 4440 bytes
- Cuando el nivel IP recibe un datagrama, identifica la interfaz de red a utilizar y la interroga sobre su MTU:
  - Compara la respuesta con la longitud del datagrama.
  - Se hace fragmentación si la longitud del datagrama es mayor que el MTU.
- El reensamblaje de datagramas IP fragmentados se produce cuando el datagrama alcanza el **destino final**:
  - Lo hace el nivel IP del destino.
  - La fragmentación es transparente al nivel de transporte.
- En la cabecera IP se almacena la información relacionada con la fragmentación IP.



# Fragmentación IP

- Cabecera IP – Campos para fragmentación





# Fragmentación IP

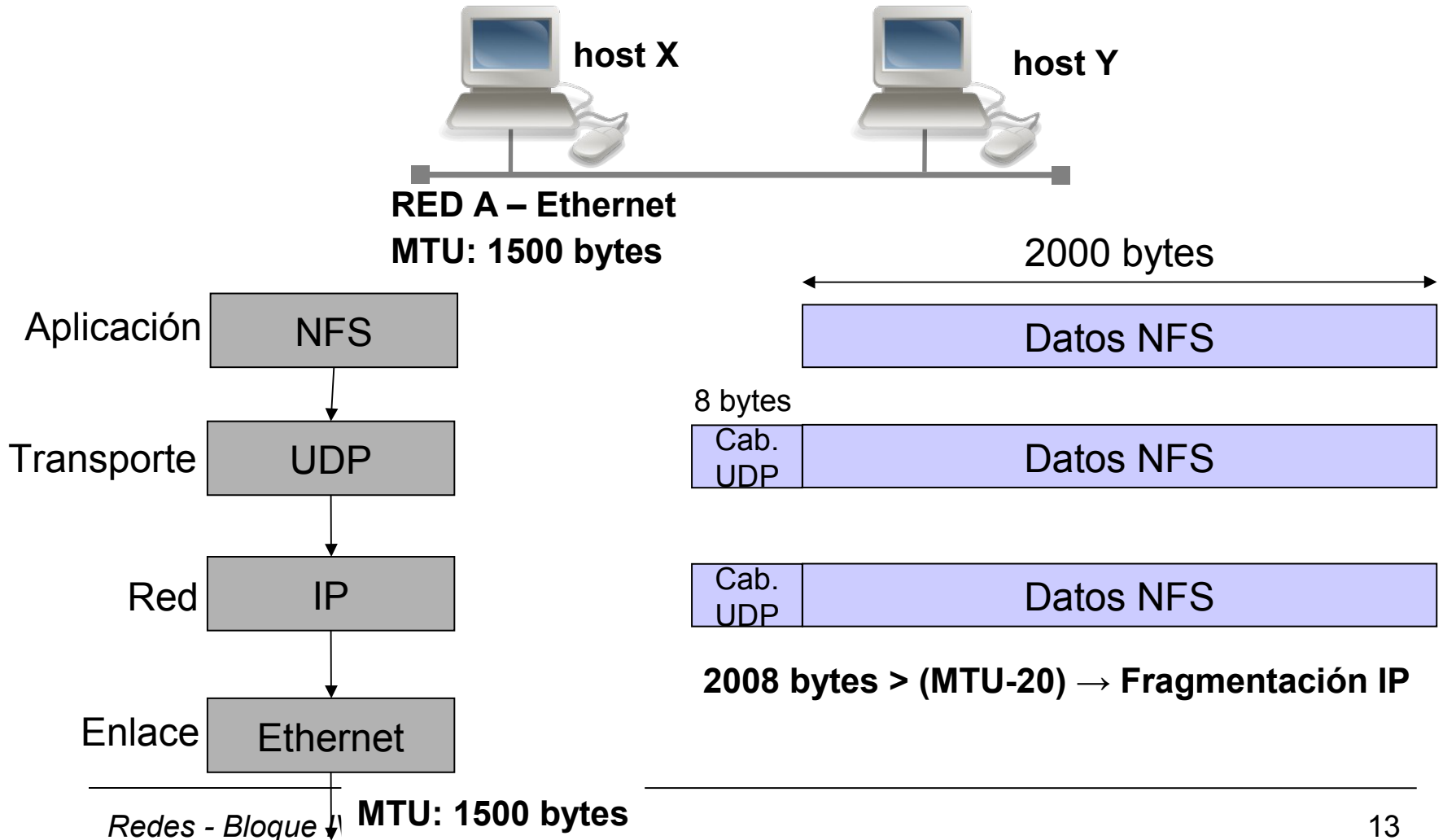
---

- **Identificación:** valor único para cada datagrama IP transmitido  
→ Todos los fragmentos de un datagrama contienen el mismo valor.
- **Flags:**
  - El primer bit está reservado.
  - Bit **DF** (Don't Fragment): a 1 si se prohíbe fragmentar el datagrama IP.
  - Bit **MF** (More Fragments): a 1 si hay más fragmentos a continuación → Se pone a 0 en el último fragmento.
- **Offset de fragmento:** desplazamiento en **múltiplos de 8 bytes** del fragmento desde el origen del datagrama original.
- **Longitud total:** se cambia la longitud total del datagrama por longitud total del fragmento.
- El tamaño de cada fragmento debe ser múltiplo de 8 bytes, excepto el último fragmento → Por el campo offset de fragmento.
- Si está activado el flag DF y es necesario fragmentar → Se genera un mensaje de error ICMP Unreachable Error (Fragmentation Required).



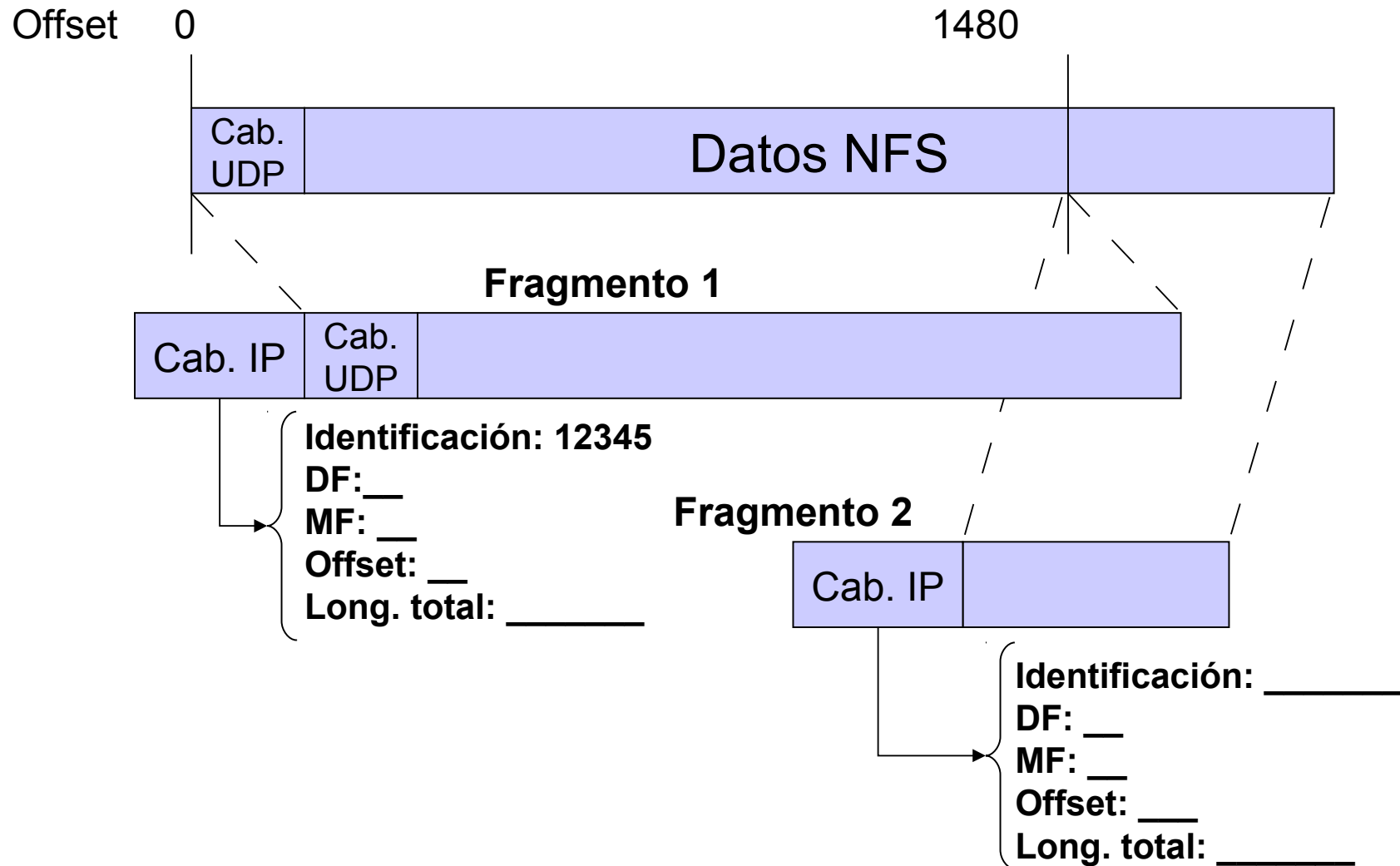
# Fragmentación IP: Ejercicio 1

- Desde el host X se envían al host Y 2000 bytes de datos NFS (utilizando el protocolo UDP).





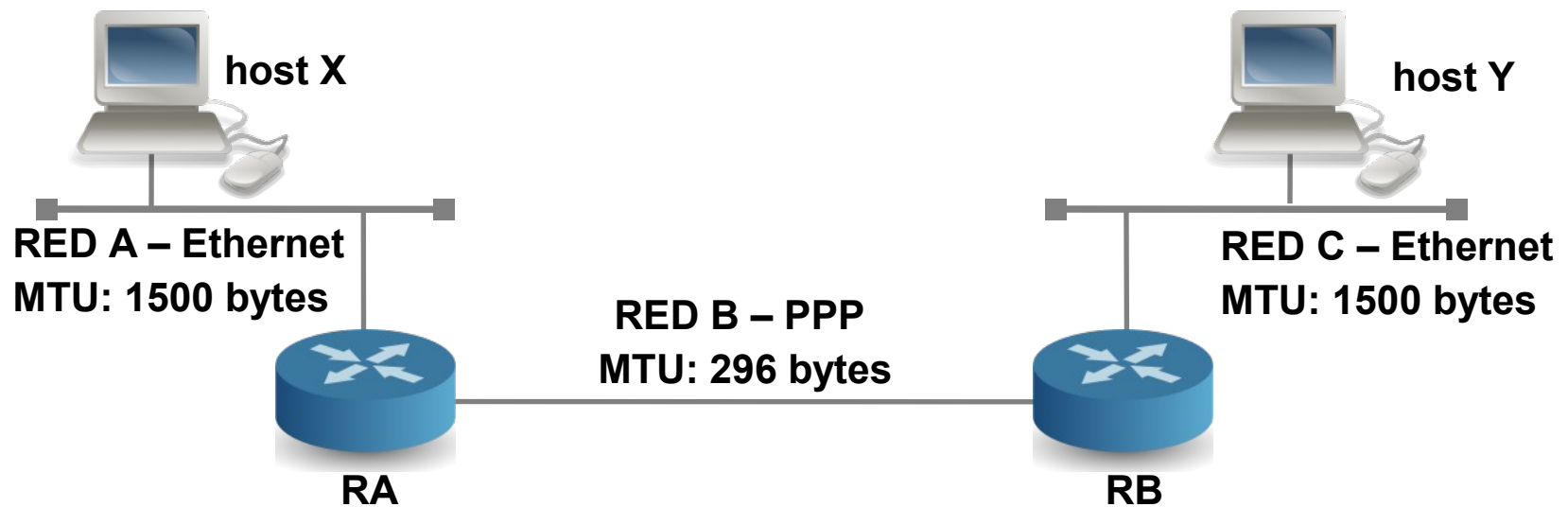
# Fragmentación IP: Ejercicio 1





# Fragmentación IP: Ejercicio 2

- Desde el host X se envían al host Y 3013 bytes de datos UDP (sin incluir la cabecera UDP).

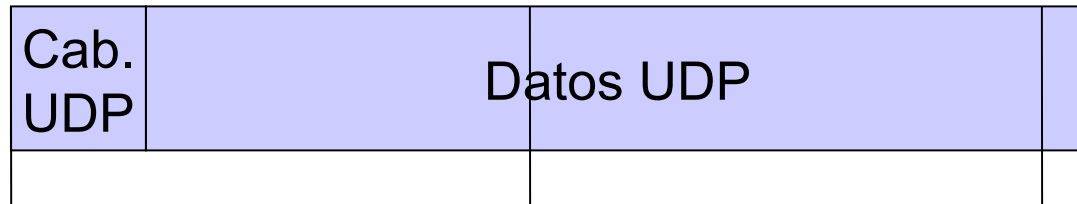




# Fragmentación IP: Ejercicio 2

8      3013 bytes

- Red A



**Fragmento 1**



Identificación: 6789

DF: \_\_ MF: \_\_

Offset: \_\_

Long. total: \_\_\_\_\_

**Fragmento 2**



Identificación: \_\_\_\_\_

DF: \_\_ MF: \_\_

Offset: \_\_\_\_\_

Long. total: \_\_\_\_\_

**Fragmento 3**



Identificación: \_\_\_\_\_

DF: \_\_ MF: \_\_

Offset: \_\_\_\_\_

Long. total: \_\_\_\_\_





# Fragmentación IP: Ejercicio 2

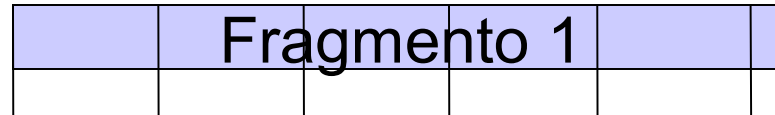
---

- Red B
  - ¿Se reagrupan los fragmentos antes de volver a fragmentarlos?
    - Sí
    - No
  - ¿Cuál es el tamaño de fragmento en la red B?
    - 276 bytes
    - 272 bytes
  - ¿Por qué?



# Fragmentación IP: Ejercicio 2

- Red B



Fragmento 1.1  
Identificación: \_\_\_\_\_  
DF: \_\_\_\_  
MF: \_\_\_\_  
Offset: \_\_\_\_  
Long. total: \_\_\_\_\_

Fragmento 1.3  
Identificación: \_\_\_\_\_  
DF: \_\_\_\_  
MF: \_\_\_\_  
Offset: \_\_\_\_  
Long. total: \_\_\_\_\_

Fragmento 1.5  
Identificación: \_\_\_\_\_  
DF: \_\_\_\_  
MF: \_\_\_\_  
Offset: \_\_\_\_  
Long. total: \_\_\_\_\_

Fragmento 1.2  
Identificación: \_\_\_\_\_  
DF: \_\_\_\_  
MF: \_\_\_\_  
Offset: \_\_\_\_  
Long. total: \_\_\_\_\_

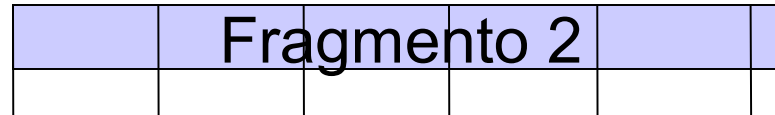
Fragmento 1.4  
Identificación: \_\_\_\_\_  
DF: \_\_\_\_  
MF: \_\_\_\_  
Offset: \_\_\_\_  
Long. total: \_\_\_\_\_

Fragmento 1.6  
Identificación: \_\_\_\_\_  
DF: \_\_\_\_  
MF: \_\_\_\_  
Offset: \_\_\_\_  
Long. total: \_\_\_\_\_



# Fragmentación IP: Ejercicio 2

- Red B



Fragmento 2.1  
Identificación: \_\_\_\_\_  
DF: \_\_\_\_  
MF: \_\_\_\_  
Offset: \_\_\_\_\_  
Long. total: \_\_\_\_\_

Fragmento 2.3  
Identificación: \_\_\_\_\_  
DF: \_\_\_\_  
MF: \_\_\_\_  
Offset: \_\_\_\_\_  
Long. total: \_\_\_\_\_

Fragmento 2.5  
Identificación: \_\_\_\_\_  
DF: \_\_\_\_  
MF: \_\_\_\_  
Offset: \_\_\_\_\_  
Long. total: \_\_\_\_\_

Fragmento 2.2  
Identificación: \_\_\_\_\_  
DF: \_\_\_\_  
MF: \_\_\_\_  
Offset: \_\_\_\_\_  
Long. total: \_\_\_\_\_

Fragmento 2.4  
Identificación: \_\_\_\_\_  
DF: \_\_\_\_  
MF: \_\_\_\_  
Offset: \_\_\_\_\_  
Long. total: \_\_\_\_\_

Fragmento 2.6  
Identificación: \_\_\_\_\_  
DF: \_\_\_\_  
MF: \_\_\_\_  
Offset: \_\_\_\_\_  
Long. total: \_\_\_\_\_



# Fragmentación IP: Ejercicio 2

---

- Red B

Fragmento 3

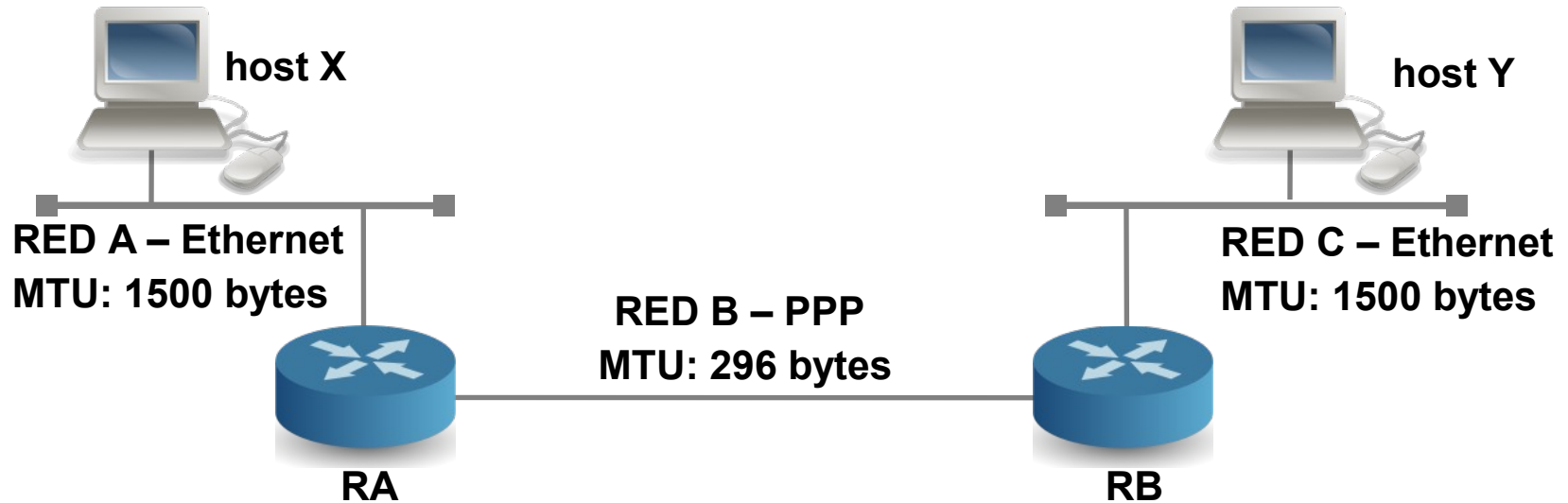
Fragmento 3  
Identificación: \_\_\_\_\_  
DF: \_\_\_\_  
MF: \_\_\_\_  
Offset: \_\_\_\_\_  
Long. total: \_\_\_\_\_

- Red C

- ¿Qué fragmentos circulan por la red C: los mismos que por la red A o por la red B?



# Fragmentación IP: Ejercicio 3



→  
SYN, <MSS 1460>

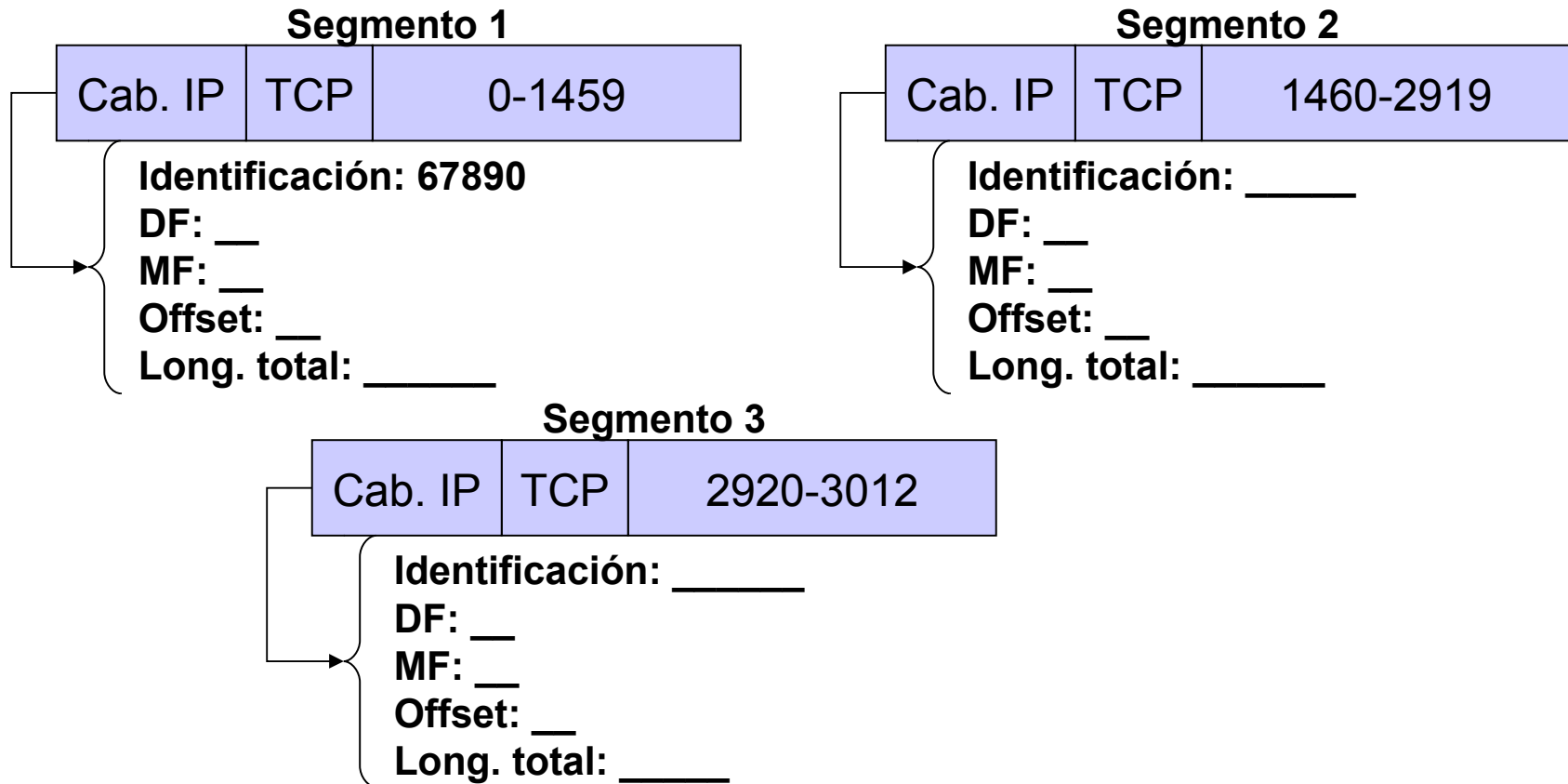
←  
SYN, <MSS 1460>

- Desde A se envían a B 3013 bytes de datos TCP (sin incluir la cabecera TCP).



# Fragmentación IP: Ejercicio 3

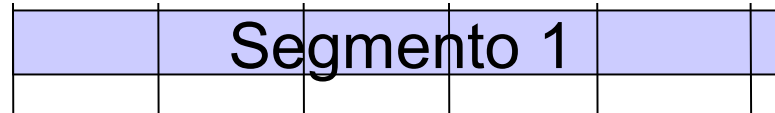
- Red A





# Fragmentación IP: Ejercicio 3

- Red B



Fragmento 1.1  
Identificación: \_\_\_\_\_  
DF: \_\_\_\_  
MF: \_\_\_\_  
Offset: \_\_\_\_  
Long. total: \_\_\_\_\_

Fragmento 1.3  
Identificación: \_\_\_\_\_  
DF: \_\_\_\_  
MF: \_\_\_\_  
Offset: \_\_\_\_  
Long. total: \_\_\_\_\_

Fragmento 1.5  
Identificación: \_\_\_\_\_  
DF: \_\_\_\_  
MF: \_\_\_\_  
Offset: \_\_\_\_  
Long. total: \_\_\_\_\_

Fragmento 1.2  
Identificación: \_\_\_\_\_  
DF: \_\_\_\_  
MF: \_\_\_\_  
Offset: \_\_\_\_  
Long. total: \_\_\_\_\_

Fragmento 1.4  
Identificación: \_\_\_\_\_  
DF: \_\_\_\_  
MF: \_\_\_\_  
Offset: \_\_\_\_  
Long. total: \_\_\_\_\_

Fragmento 1.6  
Identificación: \_\_\_\_\_  
DF: \_\_\_\_  
MF: \_\_\_\_  
Offset: \_\_\_\_  
Long. total: \_\_\_\_\_



# Fragmentación IP: Ejercicio 3

- Red B



Fragmento 1.1  
Identificación: \_\_\_\_\_  
DF: \_\_\_\_  
MF: \_\_\_\_  
Offset: \_\_\_\_  
Long. total: \_\_\_\_\_

Fragmento 1.3  
Identificación: \_\_\_\_\_  
DF: \_\_\_\_  
MF: \_\_\_\_  
Offset: \_\_\_\_  
Long. total: \_\_\_\_\_

Fragmento 1.5  
Identificación: \_\_\_\_\_  
DF: \_\_\_\_  
MF: \_\_\_\_  
Offset: \_\_\_\_  
Long. total: \_\_\_\_\_

Fragmento 1.2  
Identificación: \_\_\_\_\_  
DF: \_\_\_\_  
MF: \_\_\_\_  
Offset: \_\_\_\_  
Long. total: \_\_\_\_\_

Fragmento 1.4  
Identificación: \_\_\_\_\_  
DF: \_\_\_\_  
MF: \_\_\_\_  
Offset: \_\_\_\_  
Long. total: \_\_\_\_\_

Fragmento 1.6  
Identificación: \_\_\_\_\_  
DF: \_\_\_\_  
MF: \_\_\_\_  
Offset: \_\_\_\_  
Long. total: \_\_\_\_\_





# Fragmentación IP: Ejercicio 3

---

- Red B

## Segmento 3

Identificación: \_\_\_\_\_

DF: \_\_\_\_

MF: \_\_\_\_

Offset: \_\_\_\_\_

Long. Total: \_\_\_\_\_

- Red C
  - ¿Qué fragmentos circulan por la red C: los mismos que por la red A o por la red B?